

# Recursive constructions and their maximum likelihood decoding

Ilya Dumer and Kirill Shabunov\*

## Abstract

We consider recursive decoding techniques for RM codes, their subcodes, and newly designed codes. For moderate lengths up to 512, we obtain near-optimum decoding with feasible complexity.

## 1 Introduction

In this paper, we consider decoding algorithms that can achieve good performance and low complexity on moderate blocklengths. Our goal is to fill the void left by the best algorithms, such as optimum maximum likelihood (ML) decoding, which has unfeasible complexity even on relatively short blocks, and iterative decoding, which becomes very efficient beginning with the lengths of tens of thousands. More specifically, we wish to achieve near-optimum performance on the lengths ranging from 128 to 512, where neither of these two algorithms can yet combine good performance with low complexity.

To achieve this goal, we will use *recursive techniques*. One particular class of codes generated by (multilevel) recursion is Reed-Muller (RM) codes and their subcodes. Also, RM codes are only slightly inferior to the best codes on moderate lengths. We will see below that recursive decoding substantially outperforms other (nonexponential) algorithms known for RM codes. Our basic recursive procedure will split the *RM* code  $(r, m)$  of length  $n$  into the two constituent RM codes  $(m-1, r-1)$  and  $(m-1, r)$  of length  $n/2$ . Decoding is then relegated further to the shorter codes until we reach basic codes with feasible ML decoding. In all intermediate steps, we only recalculate the reliabilities of the newly defined symbols.

To improve decoding performance, we will also generalize recursive design. In particular, we use subcodes of RM codes and their modifications. We also use relatively short lists of code candidates in the intermediate steps of the recursion. As a result, we closely approach ML decoding performance on the blocklengths up to 512.

## 2 Reed-Muller codes

We use notation  $\left\{ \begin{smallmatrix} m \\ r \end{smallmatrix} \right\}$  for RM codes  $(n, k)$  of length  $n = 2^m$ , dimension  $k = \sum_{i=0}^r \binom{m}{i}$  and distance  $d = 2^{m-r}$ . RM codes found numerous applications thanks to fast decoding procedures. First, *majority algorithm* [6] enables feasible bounded-distance decoding and

---

\*The authors are with the College of Engineering, University of California, Riverside, CA 92521. This research was supported by the NSF grant NCR-9703844.

can even correct [3] most error patterns of weight up to  $(d \ln d)/4$  on long codes of fixed rate  $R$ .

Other efficient decoding schemes are based on recursive technique of [5] and [2]. These algorithms enable bounded distance decoding with the lowest complexity order of  $n \min(r, m - r)$  known for RM codes. Simulation results [8] show that recursive algorithms increase decoding domain of bounded distance decoding. Subsequently, these algorithms were slightly refined in [9]. It was shown that (similar to majority decoding) recursive algorithms of [5] and [2] correct most error patterns up to the weight  $(d \ln d)/4$  when used on long codes of fixed rate  $R$ .

For long low-rate RM codes of fixed order  $r$ , both majority decoding and recursive schemes correct most error patterns of Hamming weight up to  $n(1 - \varepsilon_r^{\text{maj}})/2$ , where the residual term has vanishing order

$$\varepsilon_r^{\text{maj}} \sim (m/d)^{1/2^{r+1}} \quad (1)$$

as  $m \rightarrow \infty$ . Note that (1) gives a *threshold-type* capacity that approaches the upper limit of  $n/2$ . However, degree of convergence is relatively slow even for codes  $\left\{ \begin{smallmatrix} m \\ 2 \end{smallmatrix} \right\}$ . Much better results are obtained for ML decoding. For long codes  $\left\{ \begin{smallmatrix} m \\ r \end{smallmatrix} \right\}$  of fixed order  $r$ , it is proven in [7] that ML decoding further reduces the residual term  $\varepsilon_r^{\text{maj}}$  to the order of

$$\varepsilon_r^{\text{ML}} \lesssim (\ln 4) \sqrt{m^r/n}. \quad (2)$$

### 3 Recursive structure

In essence, all recursive techniques known for RM codes are based on the *Plotkin construction*. Here the original RM code  $\left\{ \begin{smallmatrix} m \\ r \end{smallmatrix} \right\}$  is represented in the form  $(u, u+v)$ , by taking any subblock  $u$  from RM  $\left\{ \begin{smallmatrix} m-1 \\ r \end{smallmatrix} \right\}$  and any  $v$  from RM  $\left\{ \begin{smallmatrix} m-1 \\ r-1 \end{smallmatrix} \right\}$ . These two subcodes have length  $2^{m-1}$ . By continuing this process, we again obtain the shorter RM codes of length  $2^{m-2}$  and so on. Finally, we arrive at the end nodes that are repetition codes  $\left\{ \begin{smallmatrix} j \\ 0 \end{smallmatrix} \right\}$  and full spaces  $\left\{ \begin{smallmatrix} j \\ j \end{smallmatrix} \right\}$ . This is schematically shown in Fig. 1 for RM codes of length 32. In Fig. 2, we consider incomplete decomposition terminated at the biorthogonal codes  $\left\{ \begin{smallmatrix} j \\ 1 \end{smallmatrix} \right\}$  and single-parity check codes  $\left\{ \begin{smallmatrix} j \\ j-1 \end{smallmatrix} \right\}$ .

Now let  $I_r^m$  denote a block of information bits that encodes a vector  $(u, u+v)$ . It is also important that our recursion splits  $I_r^m$  into two information subblocks  $I_r^{m-1}$  and  $I_{r-1}^{m-1}$  that encode vectors  $u$  and  $v$ , respectively. Correspondingly, code dimensions satisfy the recursion  $|I_r^m| = |I_r^{m-1}| + |I_{r-1}^{m-1}|$ . In this way, the shorter information subblocks can be split again until we arrive at the end nodes. Thus, any specific codeword can be encoded from the (multiple) information strings assigned to the end nodes  $\left\{ \begin{smallmatrix} j \\ 0 \end{smallmatrix} \right\}$  or  $\left\{ \begin{smallmatrix} j \\ j \end{smallmatrix} \right\}$ . Following [2], it can be proven that recursive encoding of code  $\left\{ \begin{smallmatrix} m \\ r \end{smallmatrix} \right\}$  has complexity

$$\psi_r^m \leq n \min(r, m - r) + 1. \quad (3)$$

This observation comes from two facts. First, the end nodes  $\left\{ \begin{smallmatrix} j \\ 0 \end{smallmatrix} \right\}$  and  $\left\{ \begin{smallmatrix} j \\ j \end{smallmatrix} \right\}$  satisfy the bound (3). Second, consider the two constituent codes  $\left\{ \begin{smallmatrix} m-1 \\ r-1 \end{smallmatrix} \right\}$  and  $\left\{ \begin{smallmatrix} m-1 \\ r \end{smallmatrix} \right\}$ . Then  $(u, u+v)$  construction gives complexity  $\psi_{r-1}^{m-1} + \psi_r^{m-1} + \frac{n}{2}$  for the code  $\left\{ \begin{smallmatrix} m \\ r \end{smallmatrix} \right\}$ . Using this recursion, one can show that  $\psi_r^m$  also satisfies (3) if constituent codes do.

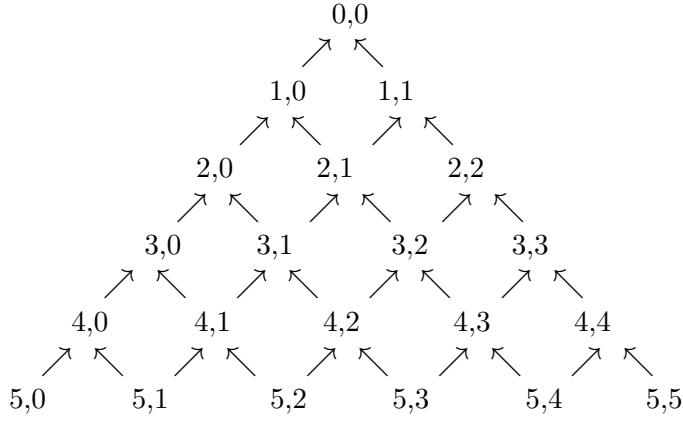


Fig. 1: Full decomposition

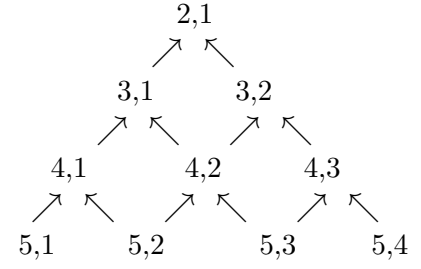


Fig. 2: Partial decomposition

## 4 New decoding techniques

Our algorithm also uses the  $(u, u+v)$  construction and relegates decoding to the two constituent RM codes. Decoder receives a block  $(\tilde{u}, \widetilde{u+v})$  that consists of two halves  $\tilde{u}$  and  $\widetilde{u+v}$  corrupted by noise. We first try to find the better protected codeword  $v$  from  $\{\tilde{u}\}_{r-1}^{m-1}$ . Then we proceed with the block  $u$  from the code  $\{\widetilde{u+v}\}_r^{m-1}$ . In a more general scheme, we repeat this recursion, by decomposing subblocks  $v$  and  $u$  further. On all intermediate steps, we only recalculate the probabilities of the newly defined symbols. Finally, we perform soft decision ML decoding once we reach the end nodes. The most important difference from the previous work [9] is that in each step we keep  $L$  most probable candidates obtained prior to this step. This difference is discussed in Section 5. In this section, we first assume that our decoding is terminated on the biorthogonal codes depicted in Fig. 2.

**Step 1.** To find a subblock  $v$  in hard-decision decoding, one would use its corrupted version  $\tilde{v} = \tilde{u} + \widetilde{u+v}$ . Using more general approach, we find the posterior probabilities of the received symbols. On the left half  $\tilde{u}$ , each symbol  $u_i$  has posterior probability

$$p'_i \stackrel{\text{def}}{=} \Pr\{u_i = 0 \mid \tilde{u}_i\}.$$

Similarly, we use the right half  $\widetilde{u+v}$  to find the posterior probability of any symbol  $u_i + v_i$ :

$$p''_i \stackrel{\text{def}}{=} \Pr\{u_i + v_i = 0 \mid \widetilde{u_i + v_i}\}.$$

Given the probabilities  $p'_i$  and  $p''_i$  of the symbols  $u_i$  and  $u_i + v_i$ , we then find the posterior probability  $p(v_i)$  of their binary sum  $v_i$ . Here we use the formula of total probability and find

$$p(v_i) \stackrel{\text{def}}{=} \Pr\{v_i = 0 \mid \tilde{u}_i, \widetilde{u_i + v_i}\} = p'_i p''_i + (1 - p'_i)(1 - p''_i). \quad (4)$$

Here we use the fact that the two original symbols  $u_i$  and  $u_i + v_i$  are independent. Also, both symbols are independently corrupted by Gaussian noise. Now we can use any soft-decision decoding that uses probabilities  $p(v_i)$  to find the most probable vector  $v$  from the  $\{\tilde{u}\}_{r-1}^{m-1}$ -code. This completes Step 1 of our algorithm. Vector  $v$  is then passed to Step 2.

**Step 2.** Now we use both vectors  $\widetilde{u+v}$  and  $v$  to estimate each symbol  $u_i$  on the right half. Assuming that  $v$  is correct, we find that each symbol  $u_i$  has posterior probability

$$p_i^\wedge \stackrel{\text{def}}{=} \Pr\{u_i = 0 \mid \widetilde{u_i + v_i}, v_i\} = \begin{cases} p''_i, & \text{if } v_i = 0, \\ 1 - p''_i, & \text{if } v_i = 1. \end{cases}$$

Now we have the two posterior probabilities  $p'_i$  and  $p_i^\wedge$  of symbols  $u_i$  obtained on both corrupted halves. By using the Bayes' rule, we find the combined estimate

$$p(u_i) \stackrel{\text{def}}{=} \Pr\{u_i = 0 \mid p'_i, p_i^\wedge\} = \frac{p'_i p_i^\wedge}{p'_i p_i^\wedge + (1 - p'_i)(1 - p_i^\wedge)}. \quad (5)$$

Finally, we perform soft decision decoding and find a subblock  $u \in \left\{ \binom{m-1}{r} \right\}$ .

Thus, procedure  $\left\{ \binom{m}{r} \right\}$  has a recursive structure that calls procedures  $\left\{ \binom{m-1}{r-1} \right\}$  and  $\left\{ \binom{m-1}{r} \right\}$ , and so on. By recalculating probabilities (4) and (5), we finally arrive at the *biorthogonal* Reed-Muller codes  $\left\{ \binom{j}{1} \right\}$  on our way to the left, or full codes  $\left\{ \binom{j}{j} \right\}$  on the way to the right. *Maximum likelihood* decoding is executed on the end nodes. Each decoding retrieves a new subset of information symbols associated with the current end node. In both cases, maximum likelihood decoding has complexity order at most  $n \log_2 n$  [4]. Simple analysis also shows that recalculating all posterior probabilities in (4) and (5) has complexity at most  $5n$ . Therefore our decoding complexity  $\Psi_r^m$  satisfies the recursion

$$\Psi_r^m \leq \Psi_{r-1}^{m-1} + \Psi_r^{m-1} + 5n.$$

This brings the overall complexity to the order of  $5n \log_2 n$  real operations. A slightly more efficient version gives complexity  $(5n \log_2 n)/2$ .

## 5 Analysis and improvements

Given the code  $\left\{ \binom{m}{r} \right\}$ , we first decode code  $\left\{ \binom{m-r+1}{1} \right\}$  followed by codes  $\left\{ \binom{m-r}{1} \right\}$ ,  $\left\{ \binom{m-r-1}{1} \right\}$ , and so on. With the exception of the leftmost and the rightmost nodes, the procedure enters each node multiple times, by taking all the paths leading to this node. It turns out that the output bit error rate (BER) significantly varies on different nodes and even on different paths leading to the same node. Therefore our first problem is to define the most error-prone paths. We start our analysis with two examples.

**Example 1.** For simplicity, assume that the all-zero codeword from the code  $\left\{ \binom{m}{r} \right\}$  is transmitted over the binary channel with crossover probability  $p = 0.9$ . Then we use formula (4) with  $p'_i = p''_i = 0.9$  to find the probability  $p(v_i)$  of correct symbol  $v_i = 0$  in the block  $v \in \left\{ \binom{m-1}{r-1} \right\}$ . From (4) we see that  $p(v_i) = 0.82$ . Subsequently, this probability  $p(v_i)$  rapidly converges to 0.5 in a few more steps. On the positive side, we note that each step gives us a better protected code that has twice the relative distance of the former one. In particular, the leftmost node  $\left\{ \binom{m-r+1}{1} \right\}$  has length  $2d$  and distance  $d$ . Its ML decoding gives asymptotically vanishing BER if the residual term  $\varepsilon_1^{\text{ML}}$  still exceeds  $(\ln 4)\sqrt{m/2d}$ , according to (2).

**Example 2.** Suppose that our original code  $\left\{ \binom{m}{r} \right\}$  from the previous example has already received the correct subblock  $v$  from the code  $\left\{ \binom{m-1}{r-1} \right\}$ . Now we need to find the remaining subblock  $u$  from the code  $\left\{ \binom{m-1}{r} \right\}$ . Given correct  $v$ , we can use (5) with  $p'_i = p_i^\wedge = 0.9$ . Then we find that symbol  $u_i$  is correct with probability  $p(u_i) \approx 0.99$ . Now we see that the probability  $p(u_i)$  rapidly increases as we move to the right. Note, however, that each new code has half the relative distance of its parent code. In other words, we subsequently improve the channel while entering the new codes with weaker correcting capabilities. Finally, the last code  $\left\{ \binom{r}{r} \right\}$  has no error protection and gives the output BER equal to its input error probability.

**Asymptotic analysis.** For AWGN channels, we assume that the all-zero codeword is transmitted as a sequence of  $+1$ s. Then we receive  $n$  independent random variables (RV)  $\widetilde{u}_i$  and  $\widetilde{u_i + v_i}$  with normal distribution  $\mathcal{N}(1, \sigma^2)$ . Accordingly, it can be readily seen that the posterior probabilities  $p'_i$  (and  $p''_i$ ) become independent RV with non-Gaussian distribution (here  $\tanh(x)$  is hyperbolic tangent):

$$p'_i = (1 + \varepsilon_i^l)/2, \quad \text{where } \varepsilon_i^l = \tanh(2\widetilde{u}_i/\sigma^2). \quad (6)$$

In the next step, we obtain the RV  $p(v_i)$  and  $p(u_i)$ . Their distributions can also be written (see [9]) in the form (6), where the residual terms are:

$$\varepsilon_i(v_i) = \varepsilon_i^l \varepsilon_i^u, \quad \varepsilon_i(u_i) = \tanh(2\widetilde{u}_i/\sigma^2 + (-1)^{v_i} 2(\widetilde{u_i + v_i})/\sigma^2). \quad (7)$$

Similar to Example 1, it can be shown that the first RV  $\varepsilon_i(v_i)$  has a smaller expectation  $\varepsilon_i(v_i)$  relative to the original estimate  $\varepsilon_i^l$ . By contrast, the second RV  $\varepsilon_i(u_i)$  has a greater expected value. Here the analysis is similar to Example 2. We also use that the newly defined RV  $\varepsilon_i(v_i)$  and  $\varepsilon_i(u_i)$  are all independent for each new step. Now consider asymptotic case of high noise power  $\sigma^2 \gg 1$ . (Note that this case is relevant to long RM codes with  $m \rightarrow \infty$  and fixed order  $r$ .) Then we use asymptotic approximations in formulas (4) and (5) and arrive at the following conclusions.

- We prove that moving to the left from  $\left\{ \begin{smallmatrix} m \\ r \end{smallmatrix} \right\}$  to  $\left\{ \begin{smallmatrix} m-1 \\ r-1 \end{smallmatrix} \right\}$  and further is equivalent to squaring our noise power (bringing it to  $\sigma^4$ , then  $\sigma^8$ , and so on), while keeping the signal energy equal to 1. By contrast, the original noise power  $\sigma^2$  is cut by half when the algorithm moves to the right (bringing it to  $\sigma^2/2$ ,  $\sigma^2/4$ , and so on).

- We prove that the left-hand movement makes our subcodes much more vulnerable. In this case, doubling the relative code distance  $d/n$  does not compensate for a stronger noise. In particular, the highest (worst) BER  $\mathcal{P}_1$  is obtained on the leftmost node  $\left\{ \begin{smallmatrix} m-r+1 \\ 1 \end{smallmatrix} \right\}$  that is decoded first. The second worst BER  $\mathcal{P}_2$  is obtained on the next decoded node  $\left\{ \begin{smallmatrix} m-r \\ 1 \end{smallmatrix} \right\}$ , and so on. Using conventional notation  $Q(x) = \int_x^\infty e^{-u^2/2} du / \sqrt{2\pi}$ , we prove that for  $m \rightarrow \infty$ :

$$\mathcal{P}_1 \sim Q(2^{(m-r)/2} \sigma^{-2^{r-1}}), \quad \mathcal{P}_2 \sim Q(2^{(m-r+1)/2} \sigma^{-2^{r-1}}). \quad (8)$$

Now we see that even two adjacent nodes give very different results, where  $\mathcal{P}_2 \sim \mathcal{P}_1^2$  for small  $\mathcal{P}_1$ . By contrast, moving to the right does not increase the output BER relative to the parent code. In this case, the lowest BER is obtained on the rightmost node  $\left\{ \begin{smallmatrix} r \\ r \end{smallmatrix} \right\}$ .

**Asymptotic comparison.** For long RM codes new recursive decoding increasingly outperforms both the majority algorithm and the former recursive techniques of [5], [8] as the block length grows. In particular, these algorithms give BER  $\mathcal{P} \sim Q(2^{(m-r)/2} \sigma^{-2^r})$ . Further, it can be shown that for long RM codes of fixed rate  $R$ , the above decoding corrects most error patterns of weight up to  $(d \ln d)/2$  thus:

- increasing  $\ln d$  times the capacity of bounded-distance decoding;
- doubling the capacity  $(d \ln d)/4$  of the former recursive technique.

**Improvements.** An important conclusion resulting from the above analysis is to set the leftmost information bits as zeros. In this way, we arrive at the subcodes of the original code  $\left\{ \begin{smallmatrix} m \\ r \end{smallmatrix} \right\}$  that are obtained by eliminating only a few least protected information bits. In particular, even eliminating the first  $m - r + 2$  information bits that form the leftmost code  $\left\{ \begin{smallmatrix} m-r+1 \\ 1 \end{smallmatrix} \right\}$ , immediately can reduce the output BER from  $\mathcal{P}_1$  to its square  $\mathcal{P}_2$  for sufficiently long codes.

Decoding performance can be further improved by using *list decoding*. To simplify the analysis, we now consider the repetition codes  $\left\{ \begin{smallmatrix} j \\ 0 \end{smallmatrix} \right\}$ . In particular, we start with the leftmost code  $\left\{ \begin{smallmatrix} m-r \\ 0 \end{smallmatrix} \right\}$  and take *both* codewords  $v = 0$  and  $\bar{v} = 1$  of length  $2^{m-r}$ . Correspondingly, we keep both posterior probabilities instead of choosing the more probable codeword. This step gives the two initial edges of a tree. Each edge is associated with a cost function equal to the log of the (corresponding) posterior probability.

Then we decode the next code  $\left\{ \begin{smallmatrix} m-r-1 \\ 0 \end{smallmatrix} \right\}$ . Note that the former codewords  $v$  and  $\bar{v}$  give different probability distributions on this node. Given  $v$  and  $\bar{v}$ , our new decoding is performed 2 times, separately for  $v$  and  $\bar{v}$ . The result is a full tree of depth 2, that has 4 new edges along with their cost functions. The next step includes 4 decodings of the code  $\left\{ \begin{smallmatrix} m-r-2 \\ 0 \end{smallmatrix} \right\}$  performed on each path of the tree. By continuing this process, we arrive at the codes  $\left\{ \begin{smallmatrix} 1 \\ 0 \end{smallmatrix} \right\}$  and  $\left\{ \begin{smallmatrix} 1 \\ 1 \end{smallmatrix} \right\}$ . We also keep accumulating the posterior probabilities of our paths. It can be seen that the resulting  $2^{m-r+2}$  paths give full biorthogonal code  $\left\{ \begin{smallmatrix} m-r+1 \\ 1 \end{smallmatrix} \right\}$ . Choosing the best path at this point becomes equivalent to the original termination at the biorthogonal codes.

To improve our decoding, we keep all  $L$  paths instead of selecting the best paths. In a more general scheme, the threshold  $L$  can be greater or smaller than  $2^{m-r+2}$ . In any case, we start at the repetition codes and keep doubling<sup>1</sup> the number of paths until  $2L$  paths are formed. After  $2L$  paths are constructed, we choose  $L$  paths with  $L$  maximum cost functions. In the end, the most probable path (that is, the path with the maximum cost function) is chosen among  $L$  paths survived at the rightmost node.

Both the simulation results and calculations show that continuous regeneration of  $L$  best candidates improves our original algorithm that selected the best path at each node. In other words, keeping the longer paths allows us to better separate the transmitted vector from the remaining candidates. As a result, we substantially reduce the overall BER even when compared to the expurgated subcodes. Note, however, that our list decoding increases complexity  $L$  times, to the order of  $Ln \log_2 n$ . To refine this scheme further, recall that the channel quality constantly improves as we move from the left to the right. Therefore, we can choose the variable threshold  $L$  that becomes smaller as our decoding progresses to the rightmost nodes. In this way, we can substantially reduce our list-decoding complexity even when  $L$  originally exceeds  $n$ .

**Simulation results.** Our results are described below in Figures 4 to 9. These figures also reflect the drastic improvements obtained when both techniques - using the subcodes and short decoding lists - were combined. The curves with  $L = 1$  show the performance of the refined version of the former recursive techniques from [5], [2], and [8]. For codes of length 256 and 512, the results are now improved by 3.5 to 5 dB at BER  $10^{-4}$ .

While using the maximum lists depicted on each figure, simulation also showed that in most cases of incorrect decoding, the erroneous result is more probable than the transmitted vector. This fact shows that our block ER (BL ER) is very close to that of ML decoding. In turn, this gives a new (experimental) bound on the BL ER of ML decoding. Also, our results substantially surpass other codes with similar parameters (see the current “world records” on <http://www331.jpl.nasa.gov/>). In Fig. 9, we summarize the results on block ER of ML decoding for RM codes  $\left\{ \begin{smallmatrix} 8 \\ 2 \end{smallmatrix} \right\}$  to  $\left\{ \begin{smallmatrix} 8 \\ 6 \end{smallmatrix} \right\}$  of length 256.

It is also interesting that subcodes usually achieve near-ML decoding using much smaller lists relative to the original RM codes. In particular, a subcode (256,78) approaches near-ML decoding using *only 32 intermediate paths*. Note that even one of the

---

<sup>1</sup>We can also increase the number of paths, say, to  $4L$  or  $8L$  on the nodes RM  $(j, j)$ .

most efficient algorithms developed in [1] uses about  $10^5$  paths for BCH codes of length 256. On the other hand, our simulation results show that codes of length 512 approach ML decoding using much bigger lists than codes of length 256. To extend the results for longer codes, we use slightly different constructions described in the next section.

## 6 More general recursive constructions

**Multiple splitting of RM codes.** Here we wish to change the original Plotkin representation. Namely, one can apply more sophisticated partitions that directly split RM codes in 4, 8, or more codes of shorter lengths. For example, by applying Plotkin construction two times, we can split the original block into four quarters  $(u, u + w_1, u + w_2, u + w_1 + w_2 + v)$ . Here  $u$  is taken from the least protected code  $\left\{ \begin{smallmatrix} m-2 \\ r \end{smallmatrix} \right\}$ , vectors  $w_1$  and  $w_2$  belong to the medium-protected code  $\left\{ \begin{smallmatrix} m-2 \\ r-1 \end{smallmatrix} \right\}$ , while  $v$  is taken from the best protected code  $\left\{ \begin{smallmatrix} m-2 \\ r-2 \end{smallmatrix} \right\}$ . Simulation performed for this construction did not improve the results presented in Figures 4 to 9.

Slightly better results were obtained for low SNR, when these four codes were combined in a different way as  $(u, u + w_1, u + w_1 + w_2, u + w_1 + w_2 + v)$ . It can be proven that for low rates the latter construction gives asymptotic improvement to our original Plotkin representation. This conclusion stems from the following facts. As before, the code  $v$  is decoded first and is most vulnerable in recursive decoding. Note also that  $v$  is obtained directly in one step, by adding the third quarter  $u + w_1 + w_2$  and the forth quarter  $u + w_1 + w_2 + v$  of our construction. Asymptotically, such a step squares the noise power, as described above. On the other hand, we reduce the length four times in each step. Accordingly, the new recursive construction reaches the leftmost nodes  $\left\{ \begin{smallmatrix} j \\ 0 \end{smallmatrix} \right\}$  in  $r/2$  steps instead of  $r$  steps used before. As a result, we can replace the former term  $\sigma^{-2^{r-1}}$  in (8) by the greater term  $\sigma^{-2^{r/2}}$ .

Despite substantial asymptotic improvements, simulation showed that these improvements start accumulating only on the lengths of 2048 and above.

**Alternating recursions.** Suppose that we use the Plotkin construction  $(u, u + v)$  in Fig. 1, but change our original code  $v$  from  $\left\{ \begin{smallmatrix} m-1 \\ r-1 \end{smallmatrix} \right\}$  to  $\left\{ \begin{smallmatrix} m-1 \\ r-2 \end{smallmatrix} \right\}$ . In other words, we move one more step to the left relative to the Plotkin construction as shown in Fig. 3. As a result, the new code  $v$  has a better error protection. This alteration also doubles the distance of code  $v$  and gives unequal error protection for the original code. On the other hand, we also reduce the overall code rate and the SNR per channel symbol (given the same SNR per information bit). This lower rate can eliminate the advantages of the better protection. To increase code rate in  $v$ , we then add extra symbols in the next splitting step. For example, we split  $v$  into codes  $\left\{ \begin{smallmatrix} m-2 \\ r-3 \end{smallmatrix} \right\}$  and  $\left\{ \begin{smallmatrix} m-2 \\ r-1 \end{smallmatrix} \right\}$ , by taking one more step to the right as presented in Fig. 3.

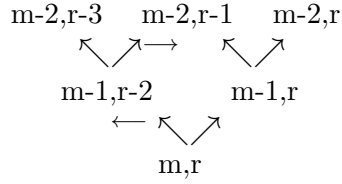


Figure 3a: Alternating decompositions

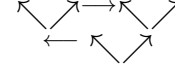


Figure 3b: Underlying structure

Note that in general alternating construction, we can no longer use RM codes. These only form the first “building blocks”, such as  $\{0^j\}$  and  $\{j^j\}$ . By contrast, various nodes  $\{i^j\}$  only label the edges/paths that correspond to our new codes. The first simulation results obtained in this direction used an  $(u, u + v)$ -combination of  $\{1^8\}$  and  $\{3^8\}$  codes instead of the original  $\{3^9\}$  code. Even this simple combination improved the original code at low SNR. More sophisticated constructions similar to the one of Fig. 3a also outperform RM codes. However, the alternating constructions that we considered to date have not yet improved the performance of subcodes presented in Figures 4 to 9.

## References

- [1] Y.S. Han, C.R.P. Hartmann, and C.K. Mohan, “Efficient heuristic search algorithms for soft-decision decoding of linear block codes,” *IEEE Trans. Inform. Theory*, vol. 44, pp. 3023-3038, 1998.
- [2] G.A. Kabatyanskii, “On decoding of Reed-Muller codes in semicontinuous channels,” *Proc. 2<sup>nd</sup> Int. Workshop “Algebr. and Combin. Coding Theory”*, Leningrad, USSR, 1990, pp. 87-91 (in Russian).
- [3] R.E. Krichevskiy, “On the Number of Reed-Muller Code Correctable Errors,” *Dokl. Soviet Acad. Sciences*, vol. 191, pp. 541-547, 1970.
- [4] S.N. Litsyn, “Fast algorithms for decoding orthogonal and related codes,” *Lecture Notes in Comp. Science*, no. 539, pp. 39-47, 1991.
- [5] S.N. Litsyn, “On decoding complexity of low-rate Reed-Muller codes,” *Proc. 9<sup>th</sup> All-Union Conf. on Coding Theory and Info. Transmission*, Part 1, Odessa, USSR, pp. 202-204, 1988 (in Russian).
- [6] I.S. Reed, “A class of multiple error correcting codes and the decoding scheme,” *IEEE Trans. Info. Theory*, vol. IT-4, pp.38-49, 1954.
- [7] V. Sidel’nikov and A. Pershakov, “Decoding of Reed-Muller codes with a large number of errors,” *Probl. Info. Transmission*, vol. 28, no. 3, pp. 80-94, 1992 (in Russian).
- [8] G. Schnabl and M. Bossert, “Soft-decision decoding of Reed-Muller codes as generalized multiple concatenated codes,” *IEEE Trans. Info. Theory*, vol. 41, pp. 304-308, 1995.
- [9] I. Dumer, “Recursive decoding of Reed-Muller codes,” *Proc. 37 Annual Allerton Conf. on Commun., Control, and Comp.*, Monticello, IL, Sept. 22-24, 1999, pp. 61-69.



FIG. 4: RM CODE (256, 37)

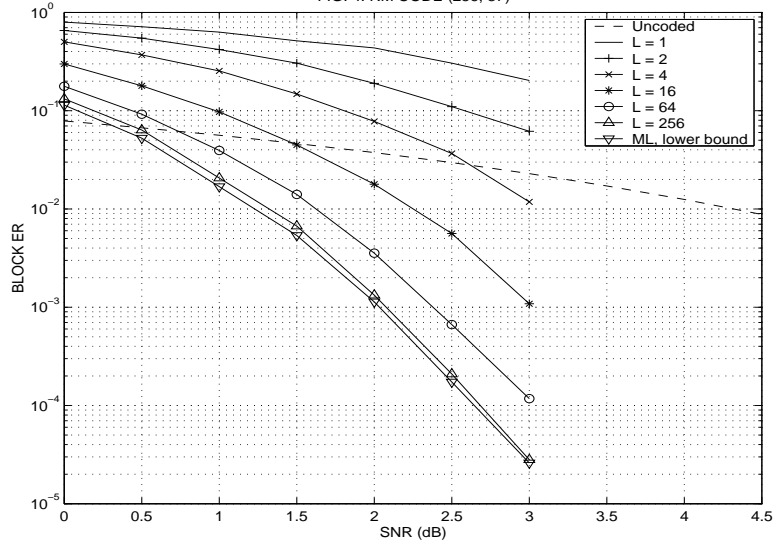


FIG. 5: SUBCODE (256, 78) OF RM CODE (256, 93)

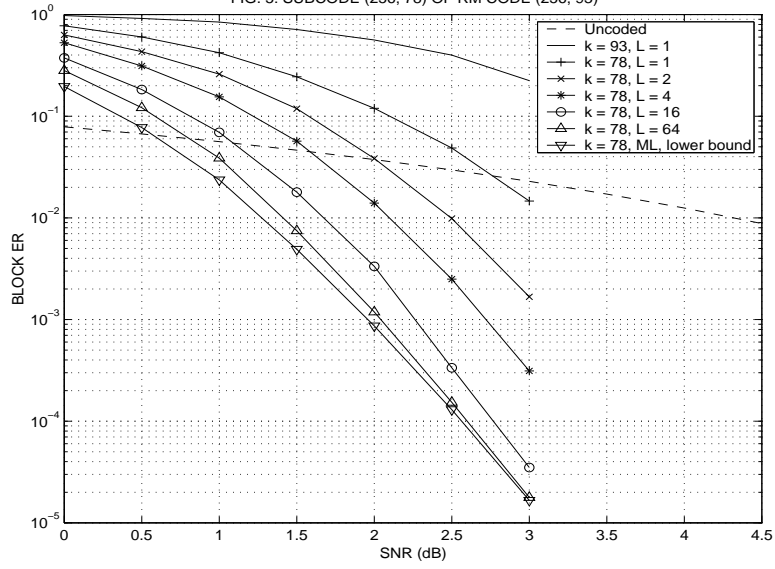


FIG. 6: SUBCODE (512, 101) OF RM CODE (512, 130)

